'Restating the Law "As It Is"': On the Tallinn Manual and the Use of Force in Cyberspace

Boer, L.J.M.

published in
Amsterdam Law Forum
2013

document version
Publisher's PDF, also known as Version of record

citation for published version (APA)
Boer, L. J. M. (2013). 'Restating the Law "As It Is"': On the Tallinn Manual and the Use of Force in Cyberspace. *Amsterdam Law Forum*, *5*(3), 4-18. http://ojs.ubvu.vu.nl/alf/article/view/323/493

AMSTERDAM LAW FORUM
VU UNIVERSITY AMSTERDAM

Article

'Restating the Law "As It Is"'[1]:

On the Tallinn Manual and the Use of Force in Cyberspace

*Lianne J.M. Boer**

Abstract

The recently published 'Tallinn Manual on the International Law Applicable to Cyber Warfare' arguably constitutes the concluding piece of a debate on the (in)applicability of the prohibition on the use of force in cyberspace. It acknowledges a framework developed by Michael Schmitt, who suggested the use of particular criteria to assess whether force has been used. This article concludes that the foundations for the suggested solutions are unsure and that, contrary to the Manual's stated goal, it adds to the existing ambiguity rather than clarifies the law on cyberattacks.

"this law is real and must be applied"[2]

Introduction

These past twenty years have witnessed a growing body of legal writing on cyberwar.[3] The notion that cyberspace might play a role in international security gained prominence after the 1991 Gulf War[4] - the first war in which "personal computers permeated all layers of

1 During the 4th CCD COE conference Michael Schmitt presented the Tallinn Manual, claiming that "it is a restatement of the law, it does not make law." CyCon 2012, Michael Schmitt: Tallinn Manual Part I. Available at http://www.youtube.com/watch?v=wY3uEo-Itso at 3:12 (accessed on 4 September 2013). In the conclusion of his article Daniel Silver uses the phrase "statement about the law as it is". D. B. Silver, 'Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter' in M.N. Schmitt & B.T. O'Donnell (eds.), 'Computer Network Attack and International Law', *International Law Studies* 2002-76, pp. 73-97, p. 94. The title of this article combines these two quotes.

* *PhD candidate Faculty of Law, VU University Amsterdam. I am highly indebted to prof. dr. W.G. Werner and prof. dr. A.R. Lodder for their guidance while writing this article.*

2 D.E. Graham, 'Cyber Threats and the Law of War', *Journal of National Security Law & Policy*, 2010-4 no. 87, pp. 87-102, p. 102.

3 The definition of cyberwar is a notorious problem. In the early days of the debate authors stated that "for now… the concept is too speculative for precise definition". See J. Arquilla & D. Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica/Washington: RAND 1997, p. 31 [originally published in *Comparative Strategy* 1993-12 no.2, pp. 141-165]. Twenty years on not much progress has been made on that point. See O.A. Hathaway et al. 'The Law of Cyber-Attack', *California Law Review* 2012-100 no. 4, pp. 817-886, p. 823.

4 The vulnerability of cyberspace came to full light after the first major virus in 1988. Anthony Rutkowski describes how "the most infamous first large-scale internet virus known as the Morris worm, took down the entire ARPA internet…". A. Rutkowski, 'Public international law of the international telecommunication instruments: cyber security treaty provisions since 1850', *info* 2011-13 no. 1, pp. 13-31, p. 19. Both Kerschischnig and Dunn Cavelty describe how cyberspace became an object of concern in international relations. See M. Dunn Cavelty, 'Unraveling the Stuxnet Effect: Of Much Persistence and Little Change in the Cyber Threats Debate', *Military and Strategic Affairs* 2011-3 no. 3, pp. 11-19, p. 12-13; G. Kerschischnig, *Cyberthreats and International Law*, The Hague: Eleven International Publishing 2012, p. 86-87. See generally on the information revolution and warfare, A. Toffler & H. Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*, London: Warner Books 1994.

command and all functions of combat operations"[5] - which led to "a watershed in military thinking about cyberwar".[6] In the almost complete absence of State practice and *opinio juris* international legal scholars played a significant role in drawing up the legal framework applicable to this "fifth domain of warfare"[7]- *inter alia* with regard to the *jus ad bellum*.[8] The legal debate arguably recently culminated in the 'Tallinn Manual on the International Law Applicable to Cyber Warfare'[9] (hereafter Manual) instigated by NATO's Cooperative Cyber Defence Centre of Excellence and created by an International Group of Experts.[10] The Manual purports to "[bring] some degree of clarity to the complex legal issues surrounding cyber operations"[11] by applying both *jus ad bellum* and *jus in bello* to war in cyberspace.[12] Composed by "distinguished international law practitioners and scholars"[13] it has been claimed to reflect "teachings of the most highly qualified publicists"[14] - an explicit reference to the sources of international law.[15] Whether justly made or not, the aggregate of this claim, the

5 C.L. Powell, 'Information-Age Warriors', *Byte* 1992-17 no. 7, p. 370.

6 Dunn Cavelty 2011, supra note 4, p. 12. The pivotal part played by the Gulf War in the perception of the possibilities of 'digital' warfare is described by Dunn Cavelty 2011, supra note 4, p. 12; C.S. Gray, 'Three Visions of Future War', *Queen's Quarterly* 1996-103 no.1, pp. 35-48, p. 40; S.P. Kanuck, 'Information Warfare: New Challenges for Public International Law', *Harvard International Law Journal* 1996-37 no.1, pp. 272-292, pp. 280-282; Kerschischnig 2012, supra note 4, p. 86; Toffler & Toffler 1994, supra note 4, in particular pp. 79-89. See for a critical note S. Biddle, 'The past as prologue: Assessing theories of future warfare', *Security Studies* 1998-8 no.1, pp. 1-74 (mainstream views on the Gulf War are portrayed on pp. 1-2).

7 "Cyberwar: War in the fifth domain" *The Economist*, 1 July 2010. Available at http://www.economist.com/node/16478792 (accessed on 4 September 2013).

8 K. Ziolkowski, '*Ius ad bellum* in Cyberspace – Some Thoughts on the "Schmitt-Criteria" for Use of Force' in C. Czosseck, R. Ottis & K. Ziolkowski (eds.) *2012 4th International Conference on Cyber Conflict: Proceedings*, Tallinn: NATO CCD COE Publications 2012, pp. 295-309, p. 297. See on the scarcity of state practice and *opinio juris* M.N. Schmitt (gen. ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge: Cambridge University Press 2013, p. 5. Dieter Fleck points out that by now 25 States have developed cyber security policies. See D. Fleck, 'Searching for International Rules Applicable to Cyber Warfare - A Critical First Assessment of the New *Tallinn Manual*', *Journal of Conflict & Security Law* 2013, advance access published 26 June 2013, doi:10.1093/jcsl/krt011, pp. 1-21, p. 5. The CCD COE website shows that the first of these policies dates back to 2008. See http://www.ccdcoe.org/328.html (accessed on 4 September 2013). Given that the scholarly debate started in the mid-1990s one could argue state practice and *opinio juris* are 'playing catch-up' with academic writing on cyberwar.

9 M.N. Schmitt (gen. ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge: Cambridge University Press 2013 (hereafter Tallinn Manual).

10 "[T]he *Tallinn Manual* is not an official document, but is only the product of a group of independent experts acting solely in their personal capacity. The Manual does not represent the views of the NATO CCD COE, its sponsoring nations, or NATO. In particular, it is not meant to reflect NATO doctrine. Nor does it reflect the position of any organization or State represented by observers." Idem, p. 11, emphasis in original.

11 Idem, p. 3.

12 Idem, p. 4. The Manual also deals with sovereignty, jurisdiction and control as well as the law of state responsibility.

13 Idem, p. 1. See on the role and function of experts, with a case study of the Tallinn Manual, O. Kessler & W. Werner, 'Expertise, Uncertainty and International Law: A study of the Tallin Manual on Cyberwarfare, *Leiden Journal of International Law* 2013-26 no. 4, *forthcoming*.

14 M.N. Schmitt, 'International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed', *Harvard International Law Journal Online* 2012-54, pp. 13-37 (Schmitt 2012a), p. 15. Available at http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf (accessed on 4 September 2013).

15 The sources of international law are "a. international conventions, whether general or particular, establishing rules expressly recognized by the contesting states; b. international custom, as evidence of a general practice accepted as law; c. the general principles of law recognized by civilized nations; d. …judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law." Statute of the International Court of Justice (hereafter ICJ Statute), 26 June 1945, 59 Stat. 1055, Art 38(1).

stature of the Manual as well as its possible impact provides sufficient reason to consider it more closely.

The publication of the Tallinn Manual is preceded by a debate that started in the mid-1990s; one that took flight after Michael Schmitt published his 'Thoughts on a Normative Framework' in 1999.[16] In this article he presented six criteria that could be applied to a cyberattack to establish whether it constitutes a violation of the prohibition on the use of force. His framework is brought to the fore by the 2013 Manual's 'Rule 11' and the accompanying Commentary on Article 2(4) of the UN Charter. This particular part of the Manual suggests that a set of criteria could be applied "to assess the likelihood that States will characterize a cyber operation as a use of force"[17] when it does not result in death and destruction - in which case it would most certainly violate Article 2(4).[18]

It is obvious that a 'use of force' is a legal qualification. Not only does it constitute an internationally wrongful act entailing the international responsibility of the State,[19] it furthermore allows the victim State to take countermeasures against the perpetrator.[20] Any criteria to establish whether force has actually been used are likewise presumably legal ones. Therefore it is rather surprising in this respect to find that the Manual not only presents the criteria as "merely factors that influence States making use of force assessments; they are not formal legal criteria"[21] but moreover claims that the Manual "is a restatement of the law, it does not make law".[22] This professed intent to restate existing law rather than proscribe new law is repeated several times, both within and outside the Manual.[23] Suggesting the use of (allegedly) non-legal criteria when making 'use of force assessments' is, however, somewhat at odds with claiming that the Manual applies "the law as it is".[24] Though the Manual only "[takes] notice"[25] of the approach originally developed by Schmitt the substantiation of these criteria in this Manual on '*the international law* applicable to cyber warfare' remains unclear. In other words, the question is how these criteria should be viewed in relation to the claims made about the nature of the Manual.

This article considers the four possible ways of viewing the status of the criteria[26]: first, they represent already existing law; second, the criteria are legal factors States *should* be taking into consideration; third, the Manual creates new law by proposing the criteria; and finally, the criteria constitute political rather than legal tools. Close analysis reveals that none of these

16 M.N. Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework', *Research Publication 1 Information Series* June 1999, pp. 1-41. Available at http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA471993 (accessed on 4 September 2013).
17 Tallinn Manual 2013, supra note 9, Commentary to Rule 11, para. 8, p. 48.
18 Ibid. A seventh and eighth criteria were added in a later stage, see below. For stylistic reasons references in this article to 'the Manual' only refer to its Introduction or those parts of it dealing with the use of force. For similar reasons, references to 'the prohibition' or 'Article 2(4)' only refer to the 'use of force', not to the other elements of Article 2(4).
19 "Every internationally wrongful act of a State entails the international responsibility of that State". See International Law Commission, Responsibility of States for Internationally Wrongful Acts, GA/Res 56/83 annex, 12 December 2001, Article 1 (Articles on State Responsibility). See also the 'Yearbook of the International Law Commission', 1980, vol. II-2, *Report of the Commission to the General Assembly on the work of its thirty-second session*, p. 53. Unless there are circumstances precluding wrongfulness; see Articles on State Responsibility, part I ch. V.
20 Articles on State Responsibility 2001, supra note 19, part III ch. II.
21 Tallinn Manual 2013, supra note 9, Commentary to Rule 11, para. 9, p. 48.
22 CyCon 2012, Michael Schmitt, supra note 1, at 3:12.
23 This is emphasized several times in the Manual, see section III of this article.
24 Silver 2002, supra note 1.
25 Tallinn Manual 2013, supra note 9, Commentary to Rule 11, para. 8, p. 48.
26 Thanks to Wouter Werner for this suggestion.

views renders a satisfactory appreciation of the relation between the criteria and the Manual. This is all the more striking given that the Manual aims to provide "some degree of clarity to the complex legal issues"[27] for a "community of nations…concerned about [the] normative ambiguity [surrounding cyber operations]".[28] This article concludes that instead of providing this clarity the Manual renders a framework strewn with uncertainty, ultimately maintaining rather than resolving, 'normative ambiguity'.

In order to develop this argument this article explores both the Manual itself as well as previous writing by Michael Schmitt, a choice that is based on the fact that the Manual refers and bears a close resemblance to his work on Article 2(4) and cyberattacks. Taking Schmitt's work into account therefore serves to broaden our understanding of the Manual. Moreover, a presentation on the Manual given by Michael Schmitt - director of the International Group of Experts behind the Tallinn Manual - at the 4th CCDCOE conference in Tallinn in 2012 has been used to more fully comprehend the ambition of the Manual's drafters.

The following section outlines what the problem is exactly when applying Article 2(4) to cyberattacks and proceeds in section II by presenting the Manual's suggestion for solving it. This section moreover looks into the background of this particular framework by considering earlier work by Michael Schmitt. The third section then focuses on the foundation for the criteria in international law. It argues that the Manual's claim of 'restating the law as it is' cannot be upheld with regard to the criteria and consequently considers alternative views. The fourth and final section provides a discussion of the conclusions drawn in this article as well as a reconsideration of the debate on the (in)applicability of Article 2(4) to cyberattacks.

I. Article 2(4), the Nature of Cyberwar and "translation problems"[29]

Article 2(4) of the UN Charter (in)famously proscribes that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations".[30] The Charter allows for two exceptions to this prohibition, namely the right to self-defence in case of an armed attack as well as the use of force authorised by the UN Security Council.[31] The question is how the prohibition on the use of force applies in cyberspace, mainly with regard to two issues.[32] First, as Article 2(4) only applies between States, the problem is how to deal with cyberattacks by non-state actors - that is, if the attack

27 Tallinn Manual 2013, supra note 9, p. 3.
28 Ibid.
29 M.C. Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)', *The Yale Journal of International Law* 2011-36 no.2, pp. 421-459, p. 437; D.B. Hollis, 'New Tools, New Rules: International Law and Information Operations' in G.J. David & T.R. McKeldin, *Ideas As Weapons: Influence and Perception in Modern Warfare*, Dulles: Potomac Books 2009, pp. 59-72, p. 63. Chapter available at http://books.google.nl/books?id=SBY1b-UrWvMC&printsec=frontcover&source=gbs_ViewAPI&redir_esc=y#v=onepage&q&f=false (accessed on 4 September 2013).
30 1945 Charter of the United Nations, 1 UNTS XVI, Article 2(4).
31 Idem, Articles 51 and 42 respectively. Article 51 states that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security." Article 42 states that "[s]hould the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations".
32 J. Barkham, 'Information Warfare and International Law on the Use of Force', *New York University Journal of International Law & Politics* 2001-34 no. 1, pp. 57-114, pp. 57-59.

can be attributed in the first place.[33] Uses of force by non-state actors traditionally have been held to be subjected to law enforcement[34] and the debate on the exercise of the right to self-defence against armed attacks by non-state actors is unresolved.[35] Through cyberspace a single hacker can create damage at levels previously mainly the preserve of States[36] and, somewhat paradoxically, this asymmetry has created a level "playing field"[37] between adversaries. Furthermore, the nature and origin of the threat are oftentimes unknown: "[t]he 'enemy' becomes a faceless and remote entity, a great unknown that is almost impossible to track."[38] As Stephen Neff points out it is precisely "the nature of the enemy [that serves] to distinguish war from…law enforcement".[39] Anonymity in cyberspace therefore not only leads to issues of attribution and doubts as to the "nature of the attack"[40], it also contributes to insecurity as to the appropriate legal framework.[41] Sean Kanuck even argues that "cyberspace…is…nearly

33 Hollis 2009, supra note 29, p. 69; Silver 2002, supra note 1, pp. 78-79; Ziolkowski 2012, supra note 8, p. 306. Hathaway et al. discuss this problem in the context of neutrality. See Hathaway et al. 2012, supra note 3, pp. 855-856.

34 T. Ruys, *'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice*, Cambridge: Cambridge University Press 2010, p. 500; see also Barkham 2001, supra note 32, p. 72. Haslam argues that law enforcement is difficult due to uncertainties with regard to attribution and the nature of the attack; the blurring "[distinction] between states of peace and armed conflict" and the range of potential harm inflicted by "information attacks". See E. Haslam, 'Information Warfare: Technological Changes and International Law', *Journal of Conflict & Security Law* 2000-5 no. 2, pp. 157-175, p. 162; Hollis 2009, supra note 29, p. 67; W.G. Sharp, *CyberSpace and the Use of Force*, Falls Church: Aegis Research Corporation 1999, p. 8. Hollis argues that "having different proscriptions for individuals and states may actually increase the danger cyberthreats pose." D.B. Hollis, 'An e-SOS for Cyberspace', *Harvard International Law Journal* 2011-52 no.2, pp. 373-432, p. 391.

35 See T. Ruys & S. Verhoeven, 'Attacks by Private Actors and the Right of Self-Defence', *Journal of Conflict & Security Law* 2005-10 no.3, pp. 289-320. The International Court of Justice (ICJ) has dealt with this issue on several occasions. See *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, I.C.J. Reports 2004, p. 136, para. 139; *Armed Activities on the Territory of the Congo* (Democratic Republic of the Congo v. Uganda), Judgment, I.C.J. Reports 2005, p. 168, paras. 146-147. For an analysis see C. Gray, *International Law and the Use of Force*, Oxford: Oxford University Press 2008, third edition, p. 202.

36 This point is emphasized by many authors. See Barkham 2001, supra note 32, mainly p. 108; S.E. Goodman, 'War, Information Technologies, and International Asymmetries', *Communications of the ACM*, 1996-39 no. 12, pp. 11-15; L.T. Greenberg, S.E. Goodman & K.J. Soo Hoo, *Information Warfare and International Law*, Washington: National Defense University Press 1998, p. 21; Hollis 2009, supra note 29, p. 67; C.C. Joyner & C. Lotrionte, 'Information Warfare as International Coercion: Elements of a Legal Framework', *European Journal of International Law* 2001-12 no. 5, pp. 825-865, p. 832; Kanuck 1996, supra note 6, p. 285; Sharp 1999, supra note 34, p. 19; Silver 2002, supra note 1, p. 73; Waxman 2011, supra note 29, p. 422.

37 Goodman 1996, supra note 36, p. 12. Goodman (pp. 12, 13) likewise states that "high-performance computing, satellite imagery, crypto technologies, and other forms of militarily useful IT, once almost exclusively available to the governments of the most powerful nation-states, are now much more available globally, including to private companies and individuals…a little high technology may provide leverage to a numerically or technologically weak combatant against a much larger or more advance adversary". See also Barkham 2001, supra note 32, pp. 66-67; Hollis 2011, supra note 34, p. 407.

38 Dunn Cavelty 2011, supra note 4, p. 13; see also Waxman 2011, supra note 29, pp. 443-444.

39 S.C. Neff, *War and the Law of Nations: A General History*, Cambridge: Cambridge University Press 2005, p. 18.

40 S.W. Brenner, '"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare', *The Journal of Criminal Law & Criminology* 2007-97 no. 2, pp. 379-476, p. 380, emphasis in original removed. See also R.W. Aldrich, 'The International Legal Implications of Information Warfare', *INSS Occasional Paper 9, Information Warfare Series*, April 1996, p. 8; Barkham 2001, supra note 32, pp. 64, 97-100; Dunn Cavelty 2011, supra note 4, p. 14; Greenberg et al. 1998, supra note 36, pp. 21-22; Haslam 2000, supra note 34, p. 162; Hollis 2011, supra note 34, pp. 377-378; Joyner & Lotrionte 2001, supra note 36, p. 828; Waxman 2011, supra note 29, i.a. p. 423fn5.

41 Hollis 2011, supra note 34, pp. 378, 405. Joyner & Lotrionte 2001, supra note 36, p. 828. More generally on the attribution issue, see Brenner 2007, supra note 40; Hollis 2011, supra note 34, in particular pp. 397-408.

impervious to regulation"[42] as war in this 'fifth domain' presents a "[change] of kind, not just of degree".[43]

Secondly - and the focus of the present article - a key question is what 'force' in cyberspace means exactly.[44] Drafted in 1945 the Charter logically did not take into account the possibility that future attacks might be conducted through codes and viruses,[45] though there does appear to be some scholarly reconciliation to the idea that the Charter does apply to war in cyberspace (see below).[46] Arguably somewhat more problematic given the interpretive history of the prohibition is the fact that cyberattacks can be both destructive as well as disturbing to daily routines[47]: cyberattacks can derail trains and steer airplanes off-course, but they can also lead to disturbances such as a temporary interruption in online banking services.[48] Moreover, there is "a much wider warspace"[49] as the vulnerability of modern societies increases with their dependence on technological infrastructures.[50]

The uneasy fit between a conventional application of Article 2(4) and cyberattacks has led legal scholars to provide different answers to the question whether the existing *jus ad bellum* is at all applicable and if so, how.[51] Some scholars answer this question in the negative and claim that the nature of cyberattacks as described above and the inadequacy of existing legal instruments to deal with them necessitates the conclusion of a "cyber-treaty".[52] Others, however, take a "law-by-analogy approach"[53] and consider cyberwar as a new yet adaptable phenomenon that can be incorporated into the current regulatory framework on the use of force. This approach has three variants, two of which shall be shortly discussed.[54] The third, instrument-based approach is left out of the discussion as "most scholars have rejected [it] as dangerously outdated".[55] It is therefore irrelevant for the current overview of mainstream approaches.

---

42 Kanuck 1996, supra note 6, p. 272.

43 Idem, p. 283.

44 Barkham 2001, supra note 32, pp. 79-95; Joyner & Lotrionte 2001, supra note 36, p. 845; Silver 2002, supra note 1, p. 74; Waxman 2011, supra note 29, pp. 426-430.

45 Hathaway et al. 2012, supra note 3, p. 840; Joyner & Lotrionte 2001, supra note 36, p. 845; Schmitt 1999, supra note 16, p. 17; Waxman 2011, supra note 29, p. 437.

46 See below.

47 Dunn Cavelty 2011, supra note 4, p. 14; Greenberg et al. 1998, supra note 36, p. 1; Haslam 2000, supra note 34, p. 162; Hollis 2009, supra note 29, p. 61; Hollis 2011, supra note 34, pp. 375, 390; Joyner & Lotrionte 2001, supra note 36, pp. 829, 835-836; Sharp 1999, supra note 34, p. 19; Silver 2002, supra note 1, p. 76; Waxman 2011, supra note 29, p. 422. The notion of "wars that [are] conducted constantly" is described rather vividly by D. Rothkopf, "The Phantom War has begun", *Foreign Policy*, Thursday, 3 November 2011. Available at http://rothkopf.foreignpolicy.com/posts/2011/11/03/the_phantom_war_has_begun (accessed on 4 September 2013).

48 Joyner & Lotrionte 2001, supra note 36, p. 841fn60. Other examples abound. See Greenberg et al. 1998, supra note 36, p. 2; Joyner & Lotrionte 2001, supra note 36, pp. 836-837.

49 Kanuck 1996, supra note 6, p. 284. See also Haslam 2000, supra note 34, p. 158.

50 Kanuck 1996, supra note 6, p. 285; this vulnerability is likewise pointed out by *inter alia* Hathaway et al. 2012, supra note 3, p. 842; Waxman 2011, supra note 29, p. 424.

51 Waxman 2011, supra note 29, p. 431; Barkham 2001, supra note 32, p. 59.

52 Hathaway et al. 2012, supra note 3; p. 877. See generally Hathaway et al. 2012, supra note 3; Hollis 2011, supra note 34; Waxman 2011, supra note 29, p. 431. Hollis 2009, supra note 29, p. 60 argues against applying existing laws altogether due to the concomitant "uncertainty…complexity…and insufficiency" such an application brings with it (emphasis in original removed). See for additional remarks section IV of this article.

53 Hollis 2009, supra note 29, p. 62.

54 Idem, p. 63: the 'instrumentality-, target- and consequentiality [effects-based] approach'.

55 Hathaway et al. 2012, supra note 3, p. 846. Hathaway et al. describe this approach in the context of cyberattacks as armed attacks; other authors discuss it with regard to the use of force. The same conclusion applies, however. See for a discussion of the instrument-based approach and Article 2(4) Hollis 2009, supra note 29, pp. 63-64.

Under the effects-based approach, a cyberattack constitutes a use of force when its effects exceed a threshold level of severity.[56] Broadly speaking, when the effects of a cyberattack are comparable to those caused by conventional means it constitutes a use of force.[57] The problem with this approach is that it leaves no "logical basis"[58] to exclude that which has traditionally always been excluded from the prohibition on the use of force: economic coercion. The fact is that economic sanctions potentially wreak havoc on a larger scale than 'conventional' use of force; the sanctions against Iraq in the early 1990s being one of the most prominent examples.[59] An effects-based approach[60] to a use of force would therefore lead to the logical inclusion of economic coercion - something States have resisted for years.[61]

This is not the only issue, however. Given the dependency of societies on cyberspace and other networks, attacks are potentially more disruptive than destructive.[62] Widespread chaos due to network malfunctions might equally threaten the 'territorial integrity or political independence' of the State. This in turn has led to the "target-based approach" under which every attack on a state's critical national infrastructure is considered a use of force.[63] A similar argument that has been put forward against the effects-based approach applies here, however: extending the scope of the prohibition to any attack on critical infrastructures, regardless of its effects, risks eroding the prohibition to include even the most minor hostile acts.[64] It seems that cyberattacks can hardly be considered in relation to Article 2(4) without simultaneously calling into question other 'use of force-categories'.[65]

Despite these shortcomings, the 'law-by-analogy approach' is likewise adopted by the Manual. The following section outlines the framework it suggests for the application of Article 2(4), followed by a critical review in section three.

II. The Tallinn Manual

The experts involved in the drafting of the Manual "[were] unanimous in [their] estimation that both the *jus ad bellum* and *jus in bello* apply to cyber operations".[66] With regard to Article

56 Its proponents include Sharp 1999, supra note 34, pp. 88-93, 102 and Ziolkowski 2012, supra note 8, p. 308. Dinstein maintains that "[i]t does not matter what specific means – kinetic or electronic – are used to bring it about, but the end result must be that violence occurs…" Y. Dinstein, *War, Aggression and Self-Defence*, Cambridge: Cambridge University Press 2012, fifth edition, p. 88.

57 Hollis 2009, supra note 29, p. 63.

58 Barkham 2001, supra note 32, p. 85.

59 See, for example, The Harvard Study Team, 'The Effect of the Gulf Crisis on the Children of Iraq', *The New England Journal of Medicine* 1991-325 no. 13, pp. 977-980.

60 The effects-based approach is described as early as 1996 by Sean Kanuck, see Kanuck 1996, supra note 6, pp. 289-292.

61 This dilemma is described most clearly by Barkham 2001, supra note 32, pp. 94-95. See also section IV of this article and fn149.

62 Barkham argues that "[d]isruption, rather than destruction, may be the sole objective in an [Information Warfare] attack." Barkham 2001, supra note 32, p. 64. See for the vulnerability of critical networks, Joyner & Lotrionte 2001, supra note 36, pp. 829-830.

63 Hollis 2009, supra note 29, pp. 63, 64.

64 Idem, p. 64. Ziolkowski adds a 'target-based' element to her effects-based approach: when critical national infrastructures are targeted and the "effects equal…the physical destruction of the respective systems", it constitutes a prohibited use of force. Ziolkowski 2012, supra note 8, p. 299.

65 Hathaway et al. 2012, supra note 3, p. 842; Waxman 2011, supra note 29, pp. 427, 453.

66 Tallinn Manual 2013, supra note 9, p. 5. According to its director, for example, the Manual "is a restatement of the law, it does not make law". CyCon 2012, Michael Schmitt, supra note 1. This emphasis

2(4), the starting point is the *Nuclear Weapons* Opinion of the International Court of Justice (ICJ) in which the Court argued *inter alia* that the prohibition on the use of force "[applies] to any use of force, regardless of the weapons employed".[67] According to the Expert Group, as a rule of customary law this facilitates the application of the prohibition to attacks in cyberspace.[68] Furthermore, in the Commentary to Rule 11 - "Definition of use of force"[69] - the Experts employ 'scale and effects', as promulgated by the ICJ in its *Nicaragua* ruling[70], as a standard for armed attacks, considering it "to be an equally useful approach when distinguishing acts that qualify as uses of force from those that do not".[71] As such, any cyberattack that leads to damage to or destruction of life and/or property amounts to a violation of the prohibition on the use of force.[72] However, the Expert Group concedes that this standard is only useful in those cases where a violation of the prohibition is obvious - somewhat irreverently the 'most-likely cases'. Not every cyberattack lends itself so easily to consideration under Article 2(4).[73] In order to regulate this grey area, the authors of the Manual suggest eight criteria that could be applied to any concrete cyberattack in order to establish whether the prohibition has been violated. Of the eight criteria - severity, immediacy, directness, invasiveness, measurability of effects, military character, State involvement and presumptive legality[74] - severity is considered by the Experts to be the most important one.[75] In line with the adopted scale and effects-standard any cyberattack that causes damage and/or destruction is probably a use of force, regardless of the 'match' with other criteria.[76] The Manual emphasises that "[these] are not formal legal criteria"[77] but "that they are merely factors that influence States making use of force assessments".[78] It furthermore adds that "in the absence of a conclusive definitional threshold [for a use of force], States contemplating cyber operations, or that are the target thereof, must be highly sensitive to the international community's probable assessment of whether the operations violate the prohibition on the use of force".[79] In other words, the list of criteria is indicative of a 'use of force assessment' only, and is not exhaustive: other factors might be taken into account appertaining to the situation at hand.[80]

The framework acknowledged in the Manual was first expounded by Michael Schmitt in 1999.[81] The starting point of his analysis is a reconstruction of the tension between Article 2(4) and cyberattacks as a problem of instruments and effects. To this end he restates the Charter's aims: to promote "international peace and security" through the prohibition on the

---

on the applicability of existing international law is repeated at several times in the Manual, e.g. on pp. 1, 5, 42.

67 *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I.C.J. Reports 1996, p. 226, para. 39; also cited in the Tallinn Manual 2013, supra note 9, para. 1, p. 42.

68 Tallinn Manual 2013, supra note 9, para.1, p. 42.

69 Idem, p. 45.

70 *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p. 14, para. 195.

71 Tallinn Manual 2013, supra note 9, Commentary to Rule 11, para. 1, pp. 45-46.

72 Idem, para. 8, p. 48. Hollis, when discussing the effects-based approach, defines it as follows: "whenever [an information operation] intends to cause effects equivalent to those produced by kinetic force (death or destruction of property), it constitutes a use of force and an armed attack." Hollis 2009, supra note 29, p. 63.

73 Tallinn Manual 2013, supra note 9, Commentary to Rule 11, para. 8, p. 48. For examples, see supra note 48.

74 Idem, para. 9, pp. 48-51.

75 Idem, p. 48.

76 Ibid.

77 Ibid.

78 Ibid.

79 Idem, para. 8, p. 48.

80 Idem, para. 10, p. 51.

81 The Manual refers to his work, see Idem, p. 48fn18.

use of force.[82] "At least since the promulgation of the Charter", Schmitt claims, "this use of force paradigm has been instrument-based."[83] The reason for this is a practical one, because even though the Charter's main concern is with the *consequences* of the use of force, these are "extraordinarily difficult to quantify or qualify….in a normatively practical manner".[84] So even though ideally 'force' would have referred to those measures producing a threshold level of death and destruction this allows for too much room for manoeuvring when deciding whether the prohibition has been violated.[85] Therefore, a "shortcut"[86] is used by considering the means with which the state measure has been executed.[87] Schmitt distinguishes between political, economic and armed coercion, where the latter poses the greatest threat to international peace and security and is therefore the only means prohibited by Article 2(4).[88] This is a reliable tool as long as instruments and effects largely coincide; in other words as long as the most serious consequences are caused by military means.[89] Cyberattacks cut through this 'congruence' as their effects can be both minor as well as very serious.[90] In other words, means and effects no longer concur. The solution lies in finding the common denominators between those consequences traditionally only caused by armed force but now potentially produced by cyberattacks as well. Schmitt's proposal is the one that is brought to the fore by the Manual: the application of a set of criteria to cyberattacks to establish whether Article 2(4) has been breached. Schmitt presented six criteria against the Manual's eight as "underlying factors driving the existing classifications"[91]; State involvement and military character are both absent from the framework proposed by Schmitt. Considered as a seventh factor Schmitt argued that "assessing State responsibility…is a practical challenge, not a normative one"[92]; though after excluding it from the framework in 1999 he added it in a later restatement of his work.[93] Military character was added in the Tallinn Manual.[94]

The framework described above can be subjected to criticism on several levels: that of the content of the criteria[95], their practical use[96] but most importantly, their status.[97] The next section will focus on this last set of criticism.

---

82 Schmitt 1999, supra note 16, p. 11.
83 Idem, p. 15.
84 Idem, p. 16.
85 Ibid.
86 Schmitt refers to this as a "cognitive shortcut", M.N. Schmitt, 'Cyber Operations and the *Jus ad Bellum* Revisited', *Villanova Law Review* 2011-56 no.3, pp. 569-606, p. 573.
87 Schmitt 1999, supra note 16, p. 16.
88 Idem, pp. 15, 17.
89 Schmitt refers to this as the "consequence-instrument congruence". Idem, p. 17.
90 Ibid.
91 Idem, p. 19.
92 Idem, p. 37fn81.
93 Schmitt 2011, supra note 86, p. 577.
94 Furthermore, the Manual changed 'presumptive legitimacy' in the original framework to 'presumptive legality'. See fn95 of this article. It also uses 'State involvement' where Schmitt used 'State responsibility'.
95 Specific criticism targets the criteria themselves, see Barkham 2001, supra note 32, mainly pp. 85-86; Silver 2002, supra note 1, pp. 89-90 and Ziolkowski 2012, supra note 8, pp. 301-308. Ziolkowski agrees to some extent with Schmitt on 'severity' as a criterion (Ziolkowski, p. 302); Silver employs a different line of reasoning and states that "examination of the criteria suggests that virtually any event of [computer network attack] can be argued to fall on the armed force side of the line, except perhaps as regards the criterion of severity, and that the criterion of severity in effect is just another way of articulating the observation that, for an event of [computer network attack] to be considered a type of force under Article 2(4), it must produce (or at least threaten to produce) personal injury or property damage similar to that caused by military weapons" (Silver, p. 89). Ziolkowski argues that 'immediacy' might have less bearing in the cyber context, as the consequences of cyberattacks may only be revealed gradually and might be temporarily concealed by victims in the private sector (Ziolkowski, p. 303). Silver argues differently; he assumes that the effects of a cyberattack will be instantaneously noticeable, and that in this respect cyberattacks and traditional uses of force are similar (Silver, pp. 89-90). With regard to 'directness'

III. On 'Restating the Law "As It Is"'

This specific part of the critique brings us to the relation between the Manual's proposed framework and its claim that the Manual itself is a "restatement of the law".[98] Starting point of the analysis is to go back to what it is these criteria are supposed to *do*. As stated above, the supposed difficulty lies in those acts that do not result in death and destruction.[99] The question is what to do with the marginal cases: hence, the criteria. They serve to distinguish between acts constituting a use of force and those that do not rise to that particular level. In other words, the aim is to facilitate a legal assessment of concrete cases that might present themselves to States.

As stated in the Introduction, the issue is how we should view the relation between the criteria and the claims made about the nature of the Manual. There are four ways of assessing this relation.[100] First, by reiterating the criteria, the Manual might indeed apply existing law to the use of force in cyberspace. It does so by referring to relevant sources, such as State practice and *opinio juris* or treaty law. A second option is that, instead, the Manual argues the criteria are how Article 2(4) *should* be translated into cyberspace; in that case the Manual would be making suggestions for the direction the law should take. As a third option, by introducing the criteria the Manual is involved in creating new law. Explicit references to one

---

Ziolkowski points out that the 'level of directness' between an attack with chemical and biological weapons is likewise weak, yet the use of these weapons "will very likely always be considered "use of [armed] force"" (Ziolkowski, p. 304). Furthermore, causation is not a legal element and thus cannot be part of a legal analysis (ibid.). Another argument is made by Silver, who states that this criterion comes down to an analysis of the level of death and destruction caused, and is therefore likewise similar to the use of armed force (Silver, p. 90). Ziolkowski argues that the 'invasiveness' of a cyberattack might likewise only be exposed gradually; furthermore, it is open to abuse if the standard used is the extent to which national interests have been infringed (Ziolkowski, p. 304). Cyberattacks and conventional uses of force are both invasive; a cyberattack requires, by whatever means, trespass into another state's territory (Silver, p. 90). Ziolkowski points out that effects might be hidden from view by the private sector; moreover cyberattacks often cause "secondary [and] tertiary…effects" (Ziolkowski, p. 305) which are harder to quantify. This puts the practical use of 'measurability' into question. Silver rejects this criterion outright as he foresees no difficulties in assessing the effects of a cyberattack (Silver, p. 90). 'Presumptive legality' proves to be a logically fallacy as a criterion: "it cannot be decided whether a particular act is indeed legal under the *ius ad bellum* by the simultaneous assertion or indication of its legality at the same time" (Ziolkowski, p. 305; though she aims the critique at the original 'presumptive legitimacy'). A similar point is made by Barkham, pp. 85-86. What is more, legitimacy constitutes a political or intuitive judgment, rather than a legal one (Ziolkowski, p. 305). The Tallinn Manual changed the original 'legitimacy' to 'legality' (Tallinn Manual 2013, supra note 9, Commentary to Rule 11, para. 9, p. 51). Silver furthermore points out that cyberattacks are in any case "presumptively illegal" under domestic laws (Silver, p. 90). Finally, the difficulty with 'State responsibility' lies in the fact that none of the available legal mechanisms is unproblematic (Ziolkowski, pp. 306-307). Though Silver, like Ziolkowski, argues that "all that is left is severity" (Silver, p, 90, emphasis in original removed), he proposes a treaty to regulate cyberattacks, see also fn144 of this article. Barkham highlights that employing just this criterion leads to overinclusion, see Barkham, i.a. pp. 59, 94-95. Schmitt replied to Ziolkowski's critique; see M.N. Schmitt, 'The 'Use of Force' in Cyberspace: A Reply to Dr Ziolkowski', in C. Czosseck, R. Ottis & K. Ziolkowski (eds.) *2012 4th International Conference on Cyber Conflict: Proceedings*, Tallinn: NATO CCD COE Publications 2012 (Schmitt 2012b), pp. 311-317.

96 A different kind of critique is aimed at the nature of the analysis: application of the criteria requires the victim state to appraise the attack when it has already passed, which few States will be willing to do. See Barkham 2001, supra note 32, p. 86. Hathaway et al. argue that the criteria are too comprehensive to be of "sufficient guidance" (Hathaway et al., p. 848) to those in power facing cyberattacks. See Hathaway et al. 2012, supra note 3, pp. 847-848.

97 Kessler & Werner 2013, supra note 13.

98 CyCon 2012, Michael Schmitt, supra note 1, at 3:12.

99 Tallinn Manual 2013, supra note 9, Commentary to Rule 11, para. 8, p. 48; Schmitt 1999, supra note 16, p. 18.

100 See fn26.

of the sources of international law would then be made to suggest that this is indeed the case. Finally, the Manual could be doing none of the above - neither applying existing law, nor making suggestions for what it ought to be, nor creating it. It might simply suggest what States could take into consideration when making these 'use of force assessments'. The following pages will discuss these four options in turn.

If the criteria, as a first option, reflect existing international law, the Manual would have had to refer to one of the sources of international law. These include treaties, customary law, general principles and "judicial decisions and the teachings of the most highly qualified publicists".[101] The criteria are supposedly founded in a reconstruction of the Charter framework - as a treaty being one of the sources of international law. As stated in section II, the validity of the criteria is based on the idea that the criteria represent "the underlying factors driving [motivating] the existing classifications"[102] in the UN Charter; they duplicate the existing framework and thereby highlight the similarities between 'traditional' uses of force and cyberattacks. In terms of the Schmitt framework, these factors represent the existing delineation between what used to be a rather one-dimensional distinction between armed coercion and other coercive means. To clarify, it is worthwhile to quote Schmitt somewhat more extensively:

> "…reference to the instrument-based shorthand facilitates greater internal consistency and predictability within the *pre-existing framework* for inter-state coercion. It allows determinations on the inclusivity of the use of force to more closely approximate the *current system* than analysis based solely on consequentiality would allow. As a result, subscription by the international community is more likely, and application should prove less disruptive and controversial. This is not to say that greater focus on core objectives, on consequentiality in its pure form, is not to be sought. It is only a recognition that until the international community casts off its current cognitive approach, community values are, for practical reasons, best advanced in terms of *that which is familiar and widely accepted*."[103]

The above citation suggests that the list of criteria does not consist of arbitrarily assembled factors, rather, they 'best advance community values' and as such they honour "the balance of the current framework".[104]

The claim that the criteria emerge from the underlying Charter-based distinctions between armed and other types of coercion would render support for the notion that the Manual applies existing law. In Schmitt's own words, the criteria are "an interpretive dilation of the use of force standard".[105] In the Manual, however, only two criteria - military character and presumptive legality - contain references to one of the sources listed above.[106] No reference is made to the UN Charter as the basis for the criteria, as Schmitt originally suggested. The question is why this substantiation in international law is limited to just these two criteria as this creates ambiguity as to their nature. Why not apply a similar method to the other six? And why is there no mention of the foundation for the criteria in the UN Charter? As an alternative, the reference to the criteria as being part of the deliberations of States might give

---

101 ICJ Statute 1945, supra note 15, Art. 38(1)(d).
102 Schmitt 1999, supra note 16, p. 19.
103 Idem, p. 20, emphases added.
104 Idem, p. 19.
105 Idem, p. 20.
106 'Presumptive legality' refers to the Lotus case of the Permanent Court of International Justice (Tallinn Manual 2013, supra note 9, p. 51fn21); 'military character' refers to the Preamble of the UN Charter (Idem, p. 50fn20). 'Invasiveness' refers to the 'Common Criteria Recognition Arrangement' (Idem, p. 49fn19) but as this Arrangement is not registered with the United Nations Treaty Collection its status is debatable. See http://www.commoncriteriaportal.org/ (accessed on 4 September 2013).

rise to the suggestion that this is State practice. This is not the position taken up in the Manual, however: it refers to the criteria as something "States are likely to consider"[107]; similarly, "States may look to [other factors]".[108] No attempt is made to abstract from these considerations to more generic State practice or *opinio juris*.[109] Though this is in line with Schmitt's later writings - in which the criteria evolved from that which 'best advances community values' to "a number of factors that would likely influence assessments by States as to whether particular cyber operations amounted to a use of force"[110] - this leaves unresolved the question of the substantiation of the criteria in existing international law.[111]

What is more, the 'Schmitt framework' relies on a very particular reconstruction of the Charter. This reconstruction centres around the assumption that the Charter's main concern is with the consequences of deleterious actions but that such a standard would be too difficult to use in practice. The question is whether this is an accurate reading of the Charter and what it is based on.[112] A completely opposite reading is likewise possible: Sean Kanuck argues that "[t]he primary concern [of, *inter alia*, Article 2(4)] is the nature of the assault, not its ramifications. Except under a very liberal reading of those terms, many of the elements of information warfare would escape interdiction under these principles of international law".[113] Such doubts as to the origins of the criteria calls into question whether they do in fact accurately reflect existing distinctions between armed coercion and other measures.[114]

With regard to this first option - that the criteria reflect existing international law - it is clear that even if one accepts Schmitt's reconstruction of the Charter's existing classifications, this particular substantiation in existing (treaty) law is lost in the Manual, nor does the Manual provide a substantiation in any of the other sources of international law.

As an alternative second option, the Manual could be making claims about what the law should look like. The argument would then be that, though not currently law, the criteria *should* become law by means of - for example - custom or treaty. However, this is not the attitude of the Manual. Rather than suggesting that States *should* take them into consideration the criteria are "[factors] States are *likely to consider* and place great weight on".[115] It is difficult to think of a formulation further removed from proscribing particular standards to States. The Manual simply states that it "took notice"[116] of the framework developed by Schmitt, which serves to "assess the likelihood that States will characterize a cyber operation as a use of force".[117] It appears to be a factual description or, perhaps, an "intuitive approach"[118] to 'use of force assessments'. This second possible appreciation of the criteria can therefore be ruled out.

---

107 Tallinn Manual 2013, supra note 9, Commentary to Rule 11, para. 9, p. 48.
108 Idem, para. 10, p. 51.
109 Kessler & Werner 2013, supra note 13.
110 Schmitt 2011, supra note 86, p. 575.
111 Kessler & Werner 2013, supra note 13.
112 Benatar urges caution against "this style of analogous reasoning". See M. Benatar, 'The Use of Cyber Force: Need for Legal Justification?', *Goettingen Journal of International Law* 2009-1 no. 3, pp. 375-396, pp. 391, 392.
113 Kanuck 1996, supra note 6, p. 289.
114 Kessler & Werner 2013, supra note 13.
115 Tallinn Manual 2013, supra note 9, Commentary to Rule 11, para. 9, p. 48, emphasis added.
116 Idem, para. 8, p. 48.
117 Ibid.
118 Kessler & Werner 2013, supra note 13. They add that "[t]his raises the question of why states would follow these intuitions regarding the *factual* behavior of states when confronted with *normative* questions regarding the scope of application of the prohibition on the use of force", emphasis in original.

If the Manual, as a third option, had suggested that the criteria create new law it would, again, have had to refer to one of the sources of international law. The work of the Group of Experts could be labelled as 'teachings of the most highly qualified publicists' and indeed is referred to as such by Schmitt himself.[119] This particular source, however, serves "as subsidiary means for the determination of rules of law"[120] - these teachings are supposed to help clarify the law, not create it. This is emphasised by Schmitt, who when presenting the Manual declared that "there is no effort to progressively develop the law".[121] In other words, there is no claim to law creation.

This rejection of the third option brings us to the fourth and final one, the possibility that the criteria amount to something completely different - simply political criteria for example. This seems to be the position taken up in the Manual itself. As indicated above the criteria are described as something 'States are likely to consider', "not exhaustive"[122] and the likelihood of them being taken into consideration as "[dependent] on the attendant circumstances".[123] This suggests that the criteria, though not fully interchangeable, are subject to change and not set in stone. As Kessler and Werner put it, the criteria "are quite *radically relativized*".[124] Secondly, the criteria are, in the words of Schmitt, "predictive tools, not normative standards"[125] - in the words of the Manual, "they are not formal legal criteria".[126] The criteria are "merely factors"[127] States take into consideration when a cyberattack occurs. These arguments serve to emphasise that the criteria constitute political rather than legal tools: they serve the choices of States rather than constitute legal guidelines for decision makers.

Though this fourth and final appreciation, in which the criteria are neither legal nor normative, seems to be the most likely one, two arguments can be brought against this conclusion. First, the application of a set of criteria underlying any legal standard has a legal effect. As argued above, a use of force entails the international responsibility of the perpetrator. Article 28 of the Articles on State Responsibility states that "[t]he international responsibility of a State which is entailed by an internationally wrongful act…involves legal consequences…"[128] These consequences include reparation for injuries and possibly countermeasures taken by the victim State.[129] To apply the criteria is in fact to come to a judgment of a certain State act and to form a legal assessment of whether the prohibition on the use of force has been violated. The claim that they are merely political (or another set of non-legal) criteria, therefore, cannot be upheld.

Secondly, the view of the criteria as propounded in the Manual - that they are 'predictive tools, not normative standards' is contradicted by earlier writing. Schmitt posits that a "*normative* evaluation of the actions that occur will centre on whether or not the [computer network attack] constituted a wrongful use of force"[130]; elsewhere he refers to these 'use of force assessments' as an "evaluative process".[131] In other words, to come to this assessment is to come to a normative statement about a certain action, and as the criteria underlie this

119 Schmitt 2012a, supra note 14, p. 15.
120 ICJ Statute 1945, supra note 15, Art. 38(1)(d).
121 CyCon 2012, Michael Schmitt, supra note 1, at 3:18.
122 Tallinn Manual 2013, supra note 9, Commentary to Rule 11, para. 10, p. 51.
123 Ibid.
124 Kessler & Werner 2013, supra note 13, emphasis in original.
125 Schmitt 2012b, supra note 95, p. 315.
126 Tallinn Manual 2013, supra note 9, Commentary to Rule 11, para. 9, p. 48.
127 Ibid.
128 Articles on State Responsibility 2001, supra note 19, Article 28.
129 Idem, Article 31(1) and part II ch. II; part III ch. II.
130 Schmitt 1999, supra note 16, p. 11, emphasis added.
131 Idem, p. 16.

assessment they cannot but be of a normative nature themselves. In this respect Schmitt's initial argument to exclude 'State responsibility' from the criteria is telling. After arguing that armed coercion is usually the prerogative of States he claims that "[h]owever, this is an issue of assessing State responsibility, not lawfulness. It is a *practical* challenge, not a *normative* one".[132] By virtue of it being a 'practical' rather than a 'normative' issue, State responsibility is excluded from the analysis.

This last reading is confirmed by other scholars. Daniel Silver, for example, praised Schmitt for his "impressive effort to delineate a *principled* basis for identifying those cases of [computer network attacks] that [sufficiently [resemble] armed force]".[133] Jason Barkham describes the reasoning behind the criteria as that they "[preserve] better consistency between evaluating computer attacks and traditional attacks".[134] As a final example, Katharina Ziolkowski is warned by Schmitt himself of "[attributing] rather more *normative* significance to [the criteria] than I do".[135]

Responding to this particular reading of his work Schmitt attributes this differing analysis to his adherence to the New Haven School, where "law…often reflects policy choices that are shaped to achieve particular values. This explains my readiness to identify influences on legal assessments that are not strictly legal in nature".[136] This amounts to a conflation of 'is' and 'ought'[137], however, a loss of the prescriptive value of law. The outcome of a 'use of force assessment' becomes entirely unpredictable as it is dependent on those factors States might consider relevant at that particular moment.[138] If the standards that make up a legal category - in this case, the use of force - are somewhat arbitrary or even entirely political in nature it is hard to see how this is still law. This is not the same as saying that States might label (or refrain from labelling) a particular incident a use of force *for political reasons* - the relevant issue is what underlies the legal qualification.

IV. Discussion

None of the four options discussed on the preceding pages results in a satisfactory appreciation of the criteria as acknowledged by the Manual. What is left is a framework strewn with ambiguity. The Manual's claim that it "examines the norms resident in the *jus ad bellum*"[139] should in all likelihood be revisited as the notion that it merely 'channels' existing law onto the cyberplane is insufficient to come to a full appreciation of the nature of the framework it 'takes notice of'. In this particular debate the 'teachings of the most highly qualified publicists' as 'subsidiary means for the determination of rules of law' might be more significant than in other debates. Considering, it is difficult to maintain that the interpretative endeavour of the Manual, more notable in light of the almost complete absence of State practice and *opinio juris*, really amounts to no more than mere law application.

This conclusion should come as no surprise. Debate on the (in)applicability of international law in general and Article 2(4) in particular is rife.[140] To illustrate, Dieter Fleck comes to the exact opposite evaluation of the Manual's success in applying existing law: "[t]he particular

132 Idem, p. 37fn81, emphasis added.
133 Silver 2002, supra note 1, p. 88, emphasis added.
134 Barkham 2001, supra note 32, p. 85, emphasis added.
135 Schmitt 2012b, supra note 95, p. 315, emphasis added.
136 Ibid.
137 Kessler & Werner 2013, supra note 13, see also the quote in fn118 of this article.
138 Idem, p. 28.
139 Tallinn Manual 2013, supra note 9, p. 42.
140 Kessler & Werner state that "questions regarding the applicability of international law to the phenomenon of cyberspace [have] been raised repeatedly". Kessler & Werner 2013, supra note 13.

achievement of the International Group of Experts", he argues, "is to have demonstrated the applicability of *lex lata* rules to new methods and means of warfare that were not even envisaged when these rules had been developed".[141] Katharina Ziolkowski on the other hand claims that in the debates on the applicability of existing *jus ad bellum* to cyberattacks "the - otherwise very commendable - distinction between *lex lata* and *lex ferenda*, as stated by many scholars, might be not always be [*sic*] appropriate".[142] Duncan Hollis even goes so far as to suggest that "[e]ven as it applies to [information operations], the existing system suffers from several, near-fatal conditions: uncertainty…complexity…and insufficiency".[143]

The possibility that existing international law is unable to deal with cyberattacks as a use of force might lend increasing support to those arguing in favour of a treaty. Several suggestions have been made, for example by Hathaway et al. who advocate a treaty containing "clear definitions of cyber-warfare and cyber-attack [as well as] guidelines for international cooperation on evidence collection and criminal prosecution".[144] The problem with drawing up a treaty is who would sign it and to what effect.[145] Not only are the means for conducting cyberattacks widely available; a significant portion of cyberattacks is carried out by non-state actors that are not necessarily under State control.[146] Furthermore, the attribution issue applies to a specific treaty on cyberattacks as much as it does to the application of Article 2(4).[147]

Ultimately, perhaps both views - the inapplicability of Article 2(4) to cyberattacks as well as (calls for) its reinterpretation - originate from the same problem. Matthew Waxman already suggests that the debate on cyberattacks and the prohibition on the use of force "echoes times past"[148]; several authors have pointed out that one encounters similar problems when discussing cyberattacks and economic coercion and their relation to Article 2(4).[149] The dichotomy described by Schmitt - the problem of instruments and effects - might run deeper than initially thought, however. Indeed, the problem the Manual is trying to solve might result from a fundamental indeterminacy of Article 2(4) which simultaneously protects and erodes its prescriptive value. In that sense, the question whether international law applies or not is not the right one to ask. The problem with applying existing law to cyberattacks results, perhaps, not so much from the particular nature of war in cyberspace but from the indeterminacy of the rule itself.[150]

---

141 Fleck 2013, supra note 8, p. 6.
142 Ziolkowski 2012, supra note 8, p. 309.
143 Hollis 2009, supra note 29, p. 60, emphasis in original removed.
144 Hathaway et al. 2012, supra note 3, p. 822. Those arguing for a cyber-treaty include Barkham 2001, supra note 32, pp. 59, 112-113; Hollis 2011, supra note 34 and Silver 2002, supra note 1, p. 94.
145 Barkham 2001, supra note 32, *inter alia* pp. 112-113.
146 Idem, pp. 59, 112.
147 Hollis 2011, supra note 34, *inter alia* p. 378; Hathaway et al. acknowledge this problem yet quote Goldsmith who says that "[s]ometimes traceback and related forensic tools can provide good-enough attribution". Hathaway et al. 2012, supra note 3, p. 884. Hollis has argued for an "e-SOS for cyberspace" under which regime States would be obliged "to assist those facing severe cyberthreats", see Hollis 2011, supra note 34, p. 408. Discussion of this alternative is beyond the scope of the present article.
148 Waxman, pp. 426, 427, 457. He argues that "[c]ompeting interpretations of Articles 2(4) and 51 have always reflected distributions of power. As a corollary, efforts to revise legal boundaries and thresholds may have re-allocative effects on power by raising or lowering the costs of using resources and capabilities that are unequally apportioned." See Waxman 2011, supra note 29, p. 448.
149 Barkham 2001, supra note 32, pp. 79-86; 94-95; Sharp 1999, supra note 34, pp. 88-93; Silver 2002, supra note 1, pp. 80-82.
150 See Lianne J.M. Boer, 'Bloody Warre, the Mistres of Debait', *forthcoming*.